STATE CORPORATION COMMISSION

Request for Information

RFI-ITD-07-005
For
Network Intrusion/Prevention/Detection and SPAM/Content Filtering/Virus Protection

Issue Date: March 16, 2007

I. Purpose for Request for Information:

The State Corporation Commission (SCC) is requesting information on your firm's ability to provide either a service provider fully managed service solution and/or a hardware/software solution to be managed internally by the SCC for Network Intrusion/Prevention/Detection Service (IPS/IDS) and SPAM/Content Filtering and Virus Scanning Services.

Suppliers should indicate their capabilities for providing either or both of the requested solutions. **All information received in response to this Request For Information (RFI) is for informational purposes only and all costs provided will be considered non-binding costs.**

II. Background:

The State Corporation Commission is located in the Tyler Building at 1300 E. Main Street, Richmond, VA, 23219. The Information Technology Division (ITD) is the SCC organizational unit responsible for the computing and networking environment, and its usage and impacts within the SCC.

Current Network Environment: SCC's core gigabit Ethernet network resides in the data center located on the 7th floor at the Tyler Building. Two Catalyst 6509 switches provide connectivity to Catalyst 3750 PoE switches located in each floors wire closets. SCC has a primary and secondary ACS server for security and network management, a WLSE server, two WLSM modules for the Catalyst 6509 switches, two PIX 515E firewalls and two 3725 CISCO Routers connected to COVANET by two T3 lines. Standard Operating system is Windows 2003 R2 Server and Windows XP on workstations. The SCC standard messaging server is Exchange 2003.

III. Requested Information and Submittal:

Responses to this RFI should include the following requested information as applicable to supplier's capability:

1. Which solution(s) are you providing a response to? (indicate by checking the appropriate solution(s)?
   - (A) Service Provider Fully Managed Solution ________
   - (B) SCC Internally Managed Hardware and Software Solution _______
   - Both A & B ________

2. If providing a response to SCC Internally Managed Hardware and Software Solution, what is the warranty period for the hardware and software?

3. What is the implementation time for the solution(s) your firm is responding to?

4. What is a fair market cost for the solution(s) your firm is capable of providing?

5. Provide a Training Plan for the Internal Solution?

6. Provide a Communications Plan for Network Attacks, Vulnerabilities, etc.

7. Provide any other information to your response that you feel is necessary for the SCC to have a thorough understanding of the solution your firm is capable of providing.

A. Service Provider Fully Managed Solution:

1. The IPS/IDS service to be fully managed by the Service Provider would provide the following:

    - All hardware/software and is responsible for hardware/software upgrade replacements during service contract.
    - Installation and configuration of Network Based IDS/IPS on SCC network segment.
    - Installation and configuration of Host Based IDS/IPS on specified Host (DMZ Servers).
    - Seven-layer traffic analysis, inspection, and prevention.
    - The ability to drop attack traffic from the network to eliminate impact.
    - 24/7 support to include monitoring and incident response resolution.
    - Notification within 15 minutes of an event of down device.
    - Flexible rule and policy settings and device tuning to reduce false positives while deterring security threats.
    - Includes automatic patching of IPS/IDS hardware and software upgrades.
    - Has centralized Secure Remote Management using WEB Portals for real time and historical reporting.
    - Sufficient storage space for reports.
    - Redundancy/failover with a 99% reliability and availability.
    - Web based reporting, automated reporting, and customized reporting features. Have the ability to export data in different formats.
    - Consults with SCC in reporting identities and blocking of network attackers
    - Training on system configuration and support procedures.
    - Training on utilization of the Report System
    - Zero Day Protection

2. The Spam/Virus Prevention service to be fully managed by the service provider would provide the following:

    - All hardware/software if applicable and is responsible for hardware/software upgrade replacements during service contract.
    - Installation and Configuration of SPAM/VIRUS Prevention Service.
    - 24/7 support/coverage.
    - The ability to add to whitelist and blacklist through centralized WEB portal if necessary
    - Detailed reporting
    - Training and procedures for support coverage.
    - Anti-virus scanning and signature updates.
    - Automatic hardware software updates.
    - Multiple layers of filtering, including whitelists, blacklists, extensive heuristic rule set, Bayesian engine, and an extensive database of known spam signatures to prevent SPAM and image based unwanted content.
    - Compatibility with the Microsoft Exchange 2003 environment.
    - Describe plans of assurance in staying current with mainstream technology.

B. SCC Internally Managed Hardware and Software Solution

1. The IPS/IDS hardware/software solution to be managed by the SCC in-house requires the following:

   - Installation/configuration all hardware/software.
   - Installation and configuration of Host Based IDS/IPS on specified Host (DMZ Servers).
   - Seven-layer traffic analysis, inspection, and prevention.
   - The ability to drop attack traffic from the network to eliminate impact.
   - Training and 24/7 technical support.
   - Flexible rule and policy settings and device tuning to reduce false positives while deterring security threats.
   - Includes automatic patching of IPS/IDS hardware and software upgrades.
   - Has centralized administration
   - Zero day protection
   - Sufficient storage space for reports.
   - Redundancy/failover with a 99% reliability and availability.
   - Web based reporting, automated reporting, and customized reporting features. Have the ability to export data in different formats.
   - Hardware/Software Maintenance

2. The SPAM/Virus Prevention hardware/software solution to be managed by the SCC in-house requires the following:

   - Installation and configuration of hardware/software.
   - Training and 24/7 technical support.
   - Detailed reporting
   - Anti-virus scanning
   - Automatic hardware/software updates.
   - Multiple layers of filtering, including whitelists, blacklists, extensive heuristic rule set, Bayesian engine, and an extensive database of known spam signatures.
   - Compatibility with the Microsoft Exchange 2003 environment.
   - Centralized administration.
   - Real-time and centralized reporting
   - The ability to protect from Image base SPAM
   - Hardware and Software Redundancy
   - Hardware/Software Maintenance

Request For Information Due until 2:00 PM Date: March 30, 2007

EMAIL, FAX OR MAIL RESPONSE TO:

State Corporation Commission
Office of Commission Comptroller
Attn: Ann Sells, VCO, CPPB
PO Box 1197
Richmond, VA 23218-1197
Ph# 804-371-2123
Fax # 804-371-9836
E-mail: ann.sells@scc.virginia.gov

Delivery Address
Tyler Bldg., 1300 E. Main Street
7th Floor Richmond, Virginia 23219

IV. Point of Contact

For questions regarding this RFI, please submit them in writing via e-mail to Ann Sells, VCO, CPPB at ann.sells@scc.virginia.gov

Questions to be submitted by **March 27, 2007.**

V. Costs

All costs submitted in response to the goods and services requested in the RFI will be considered informational and non-binding.